The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A malware detection system for determining whether an executable script is malware according to its functionality, the malware detection system comprising:

a malware signature store including at least one known malware script signature; and

a normalization module that obtains an executable script, and normalizes the executable script, thereby generating a script signature for the executable script;

and wherein the malware detection system compares the script signature for the executable script to the at least one script signature in the malware signature store to determine whether the executable script is malware.

2. The malware detection system of Claim 1, further comprising a comparison module, and wherein the comparison module compares the script signature for the executable script to the at least one script signature in the malware signature store for the malware detection system.

3. A malware detection system for determining whether an executable script is malware according to its functionality, the malware detection system comprising:

a malware signature storage means including at least one known malware script signature;

a normalization means that obtains an executable script, and normalizes the executable script, thereby generating a script signature for the executable script, wherein a script signature comprises normalized functional contents of an executable script in a format that may be compared to the normalized functional contents of other executable scripts; and

a comparison means that compares the script signature for the executable script to the at least one script signature in the malware signature storage means;

wherein the malware detection system according to the comparison performed by the comparison means, determines whether the executable script is malware.

4. A method for determining whether a computer-executable script is a malware script, the method comprising:

obtaining an executable script;

normalizing the executable script thereby generating a first script signature, wherein a script signature comprises normalized functional contents of an executable script in a format that may be compared to the normalized functional contents of other executable scripts;

comparing the first script signature to at least one script signature of known malware scripts; and

determining, based on the previous comparison, whether the executable script is a malware script.

5. A computer-readable medium bearing computer-executable instructions which, when executed on a computing device, carry out the method comprising:

obtaining an executable script;

normalizing the executable script thereby generating a first script signature, wherein a script signature comprises normalized functional contents of an executable script in a format that may be compared to the normalized functional contents of other executable scripts;

comparing the first script signature to at least one script signature of known malware scripts; and

determining, based on the previous comparison, whether the executable script is a malware script.